



AMERICAN ASSOCIATION FOR THE
ADVANCEMENT OF SCIENCE

Richard S. Nicholson
Executive Officer

FEB 12 1997

Received
2/12/97

#9
191084
1200 New York Avenue, NW
Washington, DC 20005
Tel: 202 326 6639
Fax: 202 371 9526
Internet: rnichols@aaas.org

February 7, 1997

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave., NW, Room 2705
Washington, DC 20230

Dear Ms. Crowe:

On behalf of the American Association for the Advancement of Science (AAAS), the world's largest general scientific society, I am responding to the Bureau of Export Administration's Interim Rule on the transfer of certain encryption items, published in the *Federal Register*, December 30, 1996. Before commenting directly on specific provisions of the Interim Rule, it is important to make the point that its basic thrust threatens to undermine essential features of scientific freedom and the open exchange of information that are generally acknowledged as critical to innovation in science and technology and are responsible in large part for the preeminence of America's research and development enterprise. AAAS opposes attempts by the government to restrict the communication or publication of unclassified research and technical information, efforts which we believe are inconsistent with scientific advancement. We are also concerned that certain provisions of the Interim Rule will adversely affect the effective use of information technologies in efforts to protect and promote human rights.

Many of our members in the academic community have legitimate concerns that teaching courses on cryptography appears to violate the Interim Rule if foreign students are enrolled in such courses. Such a control seems to be inadvertent, since Part 744.9 states that "mere teaching or discussion of information about cryptography ... by itself would not establish the intent described in this section, even where foreign persons are present." However, Parts 734.3(b) and 734.9 place controls on all "educational information" applying to encryption software controlled under ECCN 5D002, and "Educational information" is defined as "release by instruction in ... academic institutions." This matter requires further clarification to avoid any unnecessary chilling effect on our educational process.

Currently, part 734.3 (b)(3) of the EAR posits a difference between the paper and electronic publication of the same cryptographic materials. While it is acceptable under this provision to publish such material in a book and distribute it internationally without an export license, putting the same information on a disk and sending it abroad is subject to EAR approval. This distinction has serious ramifications for scholarly communication as many professional journals are now moving onto the Internet as electronic publications. Will cutting-edge innovations in cryptography be publishable in this new medium? Consider the following example: the full text of *Science* magazine, the major peer reviewed journal published by AAAS, is currently available in both print and electronic formats. According to the cited part in the EAR, an article accepted for publication on a new cryptographic algorithm would be acceptable in the print version of the publication. However, because the electronic version is available to people outside the U.S., to comply with EAR, the journal would either have to be published without this article or

Ms. Nancy Crowe
February 7, 1997
Page Two

substantial parts omitted. Scientific publications are crucial to the advancement of science and technology and form a primary source of communication among researchers worldwide. Restrictions that limit potential collaborations and channels of communication into new and innovative cryptographic products will not only impede scientific progress, but will also retard the evolution of a secure Global Information Infrastructure.

AAAS has encouraged the development of ethical standards by scientists to encourage responsible conduct and to establish accountability to a supportive public. The codes of professional conduct promulgated by the largest and most important U.S. professional engineering and computing societies all stress the importance of protecting established cultural and ethical norms of information privacy and data integrity. For example, the American Society of Information Science's *Code of Ethics for Information Professionals* mandates that its members "uphold each user's, provider's or employer's rights to privacy" and resist "all forms of censorship" in carrying out their responsibility "to improve, to the best of their means and abilities, the information systems in which they work or which they represent." The Interim Rule would compel these scientists and engineers -- as employees of major software and hardware computing companies -- to produce information security systems that are intentionally weak for international markets. This would create an ethical dilemma for the professional. He is bound by his responsibility to honor the ethical norms agreed upon by his profession, but as a citizen of the U.S., he is also bound by his responsibility to act according to these federal regulations. The government should avoid whenever possible creating circumstances where professionals must make such choices.

AAAS provides technical assistance to human rights groups on the design and development of information management systems for large-scale human rights data collection and analysis. This process concentrates politically volatile information in computers, such as the names of witnesses to military massacres in Guatemala who could be subjected to intimidation, harassment, or murder by those intent on preventing the public discussion and analysis of the information. Such a system must be protected by strong cryptography.

In our human rights work, we have observed the growing importance of non-governmental monitoring of state compliance with international human rights agreements as the first line of defense a civil society has against abusive regimes. By documenting and publicizing analyses of abusive behavior by governments, non-governmental human rights organizations provide a fundamental check on state repression. In order to be effective, human rights monitoring organizations must function with a high level of confidentiality. They must protect the people who give them information about state violations of human rights. Similarly, organizations must protect their own staff, many of whom may not be openly associated with the organization.

As an increasing proportion of human rights work is supported by the use of information technology, cryptographic techniques, including but not limited to encryption, have become immensely more important. Organizations that concentrate valuable, dangerous information in databases on hard disks must be able to protect them from local authorities, who may be the subjects of human rights investigations. Human rights groups communicating their findings with collaborating organizations in other countries must be able to transmit their information securely.

Ms. Nancy Crowe
February 7, 1997
Page Three

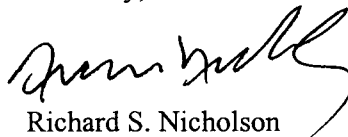
The sending organization must include sufficient information so that the receiving organization can verify the claims. If the information needed to verify the claims were intercepted, it could put the claimants in very serious danger. Using strong cryptography, human rights organizations can communicate their findings without putting informants or staff at additional risk.

These are only a few examples of the compelling need for strong cryptography by human rights organizations. The licensing provisions in the Interim Rule permit only inadequate technology for the fundamental, democratic needs of non-government human rights organizations. Part 742.15 of the Interim Rule suggests three categories of weak or unsafe encryption that are eligible for accelerated licensing: (1) includes 40-bit products called "mass market encryption software"; (2) permits key recovery products; and (3) allows non-recovery encryption items using the DES algorithm with 56-bit keys.

Provisions (1) and (3) are equally untenable for human rights purposes because they authorize only products known to be breakable with available and inexpensive technology. Provision (2), key recovery, is equally unsatisfactory for human rights organizations. If keys can be recovered by the U.S. government, why should human rights organizations whose entire function is defined by abusive governments trust that their information will remain secure? Given past and ongoing AAAS work in countries such as Haiti, Honduras, Guatemala, Turkey, and South Africa, this matter is of particular concern to us.

In view of these concerns, we urge the Bureau of Export Administration to amend the Interim Rule in favor of a more open exchange of ideas and information relating to cryptography. We believe this would advance the nation's interests in a manner consistent with the values that are responsible for America's widely admired scientific achievements and its enduring democratic traditions.

Sincerely,



Richard S. Nicholson

cc: John H. Gibbons
Mary L. Good
Orrin G. Hatch, Chair, Senate Judiciary Committee
Patrick J. Leahy, Ranking Minority Member, Senate Judiciary Committee
Jesse Helms, Chair, Senate Foreign Relations Committee
Joseph R. Biden, Jr., Ranking Minority Member, Senate Foreign Relations Committee
John McCain, Chair, Senate Commerce, Science, and Transportation Committee
Ernest F. Hollings, Ranking Minority Member, Senate Commerce, Science & Transportation Committee
Conrad Burns, Member, Senate Commerce, Science, and Transportation Committee

Ms. Nancy Crowe
February 7, 1997
Page Four

Tom Bliley, Chair, House Commerce Committee
John D. Dingell, Ranking Minority Member, House Commerce Committee
Bob Goodlatte, Member, House Commerce Committee
Henry J. Hyde, Chair, House Judiciary Committee
John Conyers, Jr., Ranking Minority Member, House Judiciary Committee
Benjamin A. Gilman, Chair, House International Relations Committee
Lee H. Hamilton, Ranking Minority Member, House International Relations Committee
F. James Sensenbrenner, Jr., Chair, House Science Committee
George E. Brown, Jr., Ranking Minority Member, House Science Committee
Kenneth C. Bass, III, Esq.
Ann Beeson, Esq.
Cindy A. Cohn, Esq.
Gino J. Scarselli, Esq.